REMARKS

Claim Changes

Claim 1 is amended to more clearly recite the claimed invention. Support for the changes can be found on page 13, lines 1-16. Thus, no new matter is added.

Claim 3 and 6 are amended to be to be consistent with claim 1 as amended.

Claim 9 is amended to clarify and simplify the language. No new matter is added.

No amendment made is related to the statutory requirements of patentability unless expressly stated herein. No amendment is made for the purpose of narrowing the scope of any claim, unless Applicant had argued herein that such amendment is made to distinguish over a particular reference or combination of references. Any remarks made herein with respect to a given claim or amendment is intended only in the context of that specific claim or amendment, and should not be applied to other claims, amendments, or aspects of Applicant's invention.

Voluntary Amendment to the Specification

Applicant has voluntarily amended the specification to replace the term "visiting member" with "mobile member" for consistency and for the purpose of clarification. No new matter is added with this amendment.

Objection to the Specification

The disclosure was objected to because of the following informalities: on page 9 there are no drawing numbers corresponding to each diagram. In response to the objection, the specification has been amended.

Objection to the Drawings

In response to the objection to FIGs. 1 and 2, Applicant has submitted replacement sheets 1/7 and 2/7. In addition, in response to the objection to FIG. 10, Applicant has amended the specification to add the reference character in the description.

Rejection under 35 U.S.C. § 112, first paragraph

The Office Action rejected claims 1-10 under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. Claim 1 is amended to be consistent with the specification. Further, Applicant respectfully submits that Applicant's specification provides support for "sending a new Visitor Encryption Key (VEK_j) to a mobile member (MM_{ij}) arriving in the corresponding group key management area ($area_j$) if there is no other mobile member (MM_{ij}) situated in the corresponding group key management area ($area_j$) and if a current Visitor Encryption Key (VEK_j) exists that has already been used to encrypt a previous Traffic Encryption Key (TEK)" on page 13, lines 1-16 of Applicant's specification. Accordingly, Applicant respectfully requests the rejection be withdrawn.

Rejection under 35 U.S.C. § 112, second paragraph

The Office Action rejected claim 9 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant has amended claim 9 amended for clarification to remedy the objection under 35 U.S.C. §112, second paragraph. Further, Applicant respectfully submits that Applicant's specification provides support for claim 9 at page 12, lines 17-23. In addition, the Office Action rejected claim 9 for insufficient antecedent basis for the limitation "said Extra Key Owner Lists" in the claim. Applicant respectfully disagrees and submits that claim 9 depends on claim 8, which further depends on claim 3, and claim 3 depends on independent claim 1. Claim 9 includes all limitations of claims 8, 3, and 1. Claim 1 includes the limitation "Extra Key Owner Lists." See claim 1, line 10. Therefore, claim 9 has sufficient antecedent basis for the limitation "said Extra Key Owner Lists." Accordingly, Applicant respectfully requests the rejection be withdrawn.

Rejection of claims 1-7 under 35 U.S.C. § 102(e) as being anticipated by US 6,584,566 (Hardjono)

Applicant respectfully traverses the rejection of claims 1-7.

Applicant respectfully submits that Hardjono does not anticipate, either expressly or inherently, each and every element as set forth in independent claim 1. For example, independent claim 1 recites "said local Group Controller Key Servers (GCKSi, GCKSj) constitute Extra Key Owner Lists (EKOLi, EKOLj) for said group key management areas (areai, areaj) that distinguish group members (MMi, MMj) possessing Key Encryption Keys (KEKi, KEKj) and situated in the corresponding group key management area (areai, areaj) from group members (MMij) possessing Key Encryption Keys (KEKi) that were situated in the corresponding group key management area (areai) but are visiting another area (areaj)" which is not anticipated either expressly or inherently, in Hardjono.

Hardjono is directed to "A method and apparatus for distributed group key management for multicast security. According to one aspect of the invention, an initiator key server distributes to a plurality of key servers a first key set including an initial common group key and a replacement common group key. The initial common group key, but not the replacement common group key, is initially distributed to clients of the plurality of key servers that are currently members of a multicast group as a current common group key for multicast messages. Responsive to a need to re-key the current common group key of the multicast group, each of the key servers subsequently distributes to their clients that are currently members of the multicast group the previously distributed replacement common group key as the current common group key." (Hardjono, Abstract).

Applicant respectfully disagrees with the statement in item 8, page 6, of the Office Action dated October 02, 2008 that Hardjono describes extra key owner lists that distinguish group members. According to Applicant's claim, "local Group Controller Key Servers (GCKSi, GCKSj) constitute Extra Key Owner Lists (EKOLi, EKOLj) for said group key management areas (areai, areaj) that distinguish group members (MMi, MMj) possessing Key Encryption Keys (KEKi, KEKj) and situated in the corresponding group key management area (areai, areaj) from group members (MMij) possessing Key Encryption Keys (KEKi) that were situated in the corresponding group key management area (areai) but are visiting another area (areaj)." In contrast, Hardjono merely discloses that a key server provides a new domain key to the initiator key server when a member leaves the key server. See Hardjono, column 9, lines 39-45. Hardjono

nowhere discloses an extra key owner list that distinguishes between group members. Therefore, Hardjono does not disclose "said local Group Controller Key Servers (GCKSi, GCKSj) constitute Extra Key Owner Lists (EKOLi, EKOLj) for said group key management areas (areai, areaj) that distinguish group members (MMi, MMj) possessing Key Encryption Keys (KEKi, KEKj) and situated in the corresponding group key management area (areai, areaj) from group members (MMij) possessing Key Encryption Keys (KEKi) that were situated in the corresponding group key management area (areai) but are visiting another area (areaj)" as recited in independent claim 1.

Further, Applicant respectfully disagrees with the statement in item 8, page 6, of the Office Action that Hardjono describes forwarding traffic encryption keys to group members visiting the respective group key management areas encrypted using a Visitor Encryption Key. It appears that the Office Action equates Applicant's group members (MMij) visiting the respective group key management areas to Hardjono's client (or new member). This is a mischaracterization. According to Applicant's claim, a key server "forward[ing]es said Traffic Encryption Keys (TEK) to group members (MMij) visiting the respective group key management areas (areaj) encrypted using a Visitor Encryption Key (VEKj) that is specific to the respective local Group Controller Key Server (GCKSj) and is different from said Key Encryption Key (KEKj)." Applicant's visiting member is a group member that is visiting a group key management area within a multicast group. In contrast, Hardjono's client is an external device, which joins a multicast group. See Hardjono, col. 10, lines 1-9. Hardjono's client is not a group member visiting from one area to another within the same multicast group. Therefore, Hardjono does not disclose "forwarding said Traffic Encryption Keys (TEK) to group members (MMij) visiting the respective group key management areas (areaj) encrypted using a Visitor Encryption Key (VEKj) that is specific to the respective local Group Controller Key Server (GCKSj) and is different from said Key Encryption Key (KEKj)" as recited in independent claim 1.

Furthermore, Applicant respectfully disagrees with the statement in item 8, page 6, of the Office Action that Hardjono describes sending a new visitor encryption key to visiting group members if no other mobile member exists or if a current visitor encryption key has been used to

encrypt a previous traffic encryption key. It appears that the Office Action equates Applicant's sending a new visitor encryption key to Hardjono's establishing a member key with a new member. However, according to Applicant's amended claim, a key server "send[ing]s a new Visitor Encryption Key (VEKj) to a mobile member (MMij) arriving in the corresponding group key management area (areaj) if there is no other mobile member (MMij) situated in the corresponding group key management area (areaj) and if a current Visitor Encryption Key (VEKj) exists that has already been used to encrypt a previous Traffic Encryption Key (TEK)." In contrast, Hardjono merely discloses that a [new] member key is associated with a new member joining the key server. See Hardjono, col. 10, lines 27-35. Hardjono nowhere discloses that a new key is generated depending upon certain conditions. Therefore, Hardjono does not disclose "sending a new Visitor Encryption Key (VEKj) to a mobile member (MMij) arriving in the corresponding group key management area (areaj) if there is no other mobile member (MMij) situated in the corresponding group key management area (areaj) and if a current Visitor Encryption Key (VEKj) exists that has already been used to encrypt a previous Traffic Encryption Key (TEK)" as recited in independent claim 1.

In view of the foregoing, Applicant respectfully submits that Hardjono does not disclose "Extra Key Owner Lists (EKOLi, EKOLj) for said group key management areas (areai, areaj) that distinguish group members (MMi, MMj)," "forwarding said Traffic Encryption Keys (TEK) to group members (MMij) visiting the respective group key management areas (areaj) encrypted using a Visitor Encryption Key (VEKj)," and "sending a new Visitor Encryption Key (VEKj) to a mobile member (MMij) arriving in the corresponding group key management area (areaj) if there is no other mobile member (MMij) situated in the corresponding group key management area (areaj) and if a current Visitor Encryption Key (VEKj) exists that has already been used to encrypt a previous Traffic Encryption Key (TEK)." Applicant therefore submits that claim 1 not anticipated by Hardjono, and therefore the rejection of claim 1 under 35 USC 102(e) should be withdrawn. Applicant requests that claim 1 may now be passed to allowance.

Dependent claims 2-7 depend from, and include all the limitations of independent claim 1. Therefore, Applicant respectfully requests reconsideration of dependent claims 2-7 and requests the withdrawal of the rejection.

Rejection of claims 8-10 under 35 U.S.C. § 103 (a) as being unpatentable over US 6,584,566 (Hardjono) in view of Non Patent Literature "Secure Group Communications for Wireless Networks" pages 113-117 (Decleene)

As mentioned above, Applicant respectfully submits that Hardjono does not disclose "Extra Key Owner Lists (EKOLi, EKOLj) for said group key management areas (areai, areaj) that distinguish group members (MMi, MMj)," "forwarding said Traffic Encryption Keys (TEK) to group members (MMij) visiting the respective group key management areas (areaj) encrypted using a Visitor Encryption Key (VEKj)," and "sending a new Visitor Encryption Key (VEKj) to a mobile member (MMij) arriving in the corresponding group key management area (areaj) if there is no other mobile member (MMij) situated in the corresponding group key management area (areaj) and if a current Visitor Encryption Key (VEKj) exists that has already been used to encrypt a previous Traffic Encryption Key (TEK)." Since Harjono does not teach or suggest above-stated elements of independent claim 1, the combination of Hardjono with Decleene also fails to disclose Applicant's claimed invention. Applicant respectfully requests withdrawal of the rejection of claims 8-10 under 35 USC 103(a). Applicant requests that claims 8-10 now be passed to allowance.

Conclusion

Applicant has reviewed the other references of record and believes that Applicant's claimed invention is patentably distinct and nonobvious over each reference taken alone or in combination. Applicant respectfully requests that a timely Notice of Allowance be issued in this case. Such action is earnestly solicited by the Applicant. Should the Examiner have any questions, comments, or suggestions, the Examiner is invited to contact the Applicant's attorney or agent at the telephone number indicated below.

Please charge any fees that may be due to Deposit Account 502117, Motorola, Inc.

Respectfully submitted,

December 23, 2008

By: /Barbara R. Doutre/
Barbara R. Doutre
Attorney for Applicant
Registration No. 39,505
Tel. No. 954-723-6449
Fax No. 847-576-3750
Email: docketing.us@motorola.com

Motorola, Inc.
1303 East Algonquin Road
IL01 – 3rd Floor
Schaumburg, Illinois 60196
Customer Number: 24273